Exponential Sums Algorithm based on Optical Interference: Factorization of arbitrary large numbers in a single run

Vincenzo Tamma[1,2], Heyi Zhang[1], Xuehua He[1], Augusto Garuccio [2], and Yanhua Shih[1]
[1] *Department of Physics, University of Maryland, Baltimore County, Baltimore, Maryland 21250, USA,* [2] *Dipartimento Interateneo di Fisica, Università degli Studi di Bari, 70100 Bari, Italy*

This article presents a new factorization algorithm based on the implementation of exponential sums using optical interference and exploiting the spectrum of the light source. Such a goal is achievable with the use of two different kinds of optical interferometers with variable optical paths: a liquid crystal grating and a generalized symmetric Michelson interferometer. This algorithm allows, for the first time, to find, in a single run, all the factors of an arbitrary large number N.

The factorization of large numbers N is a lot more difficult than the reverse operation of multiplying large prime numbers. This difficulty is at the basis of encryption systems [1]. A more recent approach to factorization, proposed by W. Schleich, exploits the periodic properties of truncated exponential sums [2, 3, 4] of order j:

$$\mathcal{A}_N^{(M,j)}(\ell) = \frac{1}{M+1}\sum_{m=0}^{M} \exp\left[-2\pi i\, m^j \frac{N}{\ell}\right], \qquad (1)$$

where $M+1$ is the number of phase terms in the sum (M is called the truncation parameter), N is the number to be factored, and j and l are positive integers, with $j > 1$ and $1 \leq \ell \leq \sqrt{N}$, respectively. For $j = 2$, the truncated exponential sum reduces to a truncated Gauss sum [2]. If ℓ is a factor of N, all the terms interfere constructively and the truncated exponential sum assumes its maximum value, i.e. 1. On the other hand, if ℓ is not a factor of N, the truncated exponential sum assumes a value less than one, because of the destructive interference caused by the rapid oscillation of the phases terms of order j in Eq. (1). Obviously, the more terms involved in the sum (i.e. the larger the truncation parameter M), the better we can distinguish between factors and non factors. It turns out that one needs at least $M \sim \sqrt[2j]{N}$ terms in order to discriminate factors from non factors [4].

Truncated Gauss sums have been reproduced using different techniques [5, 6, 7, 8]. Unfortunately, all these past experimental realizations present two common problems. The first one is that there is only one knob (one physical parameter) to vary the global ratio N/ℓ: the ratio N/ℓ is known before the experiment is run. The second problem is that it is necessary to run the experiment for each possible trial factor ℓ, to find out which ones are the factors.

We wish to present a new approach, based on optical interference, which allows, for the first time, to obtain all the factors of a large number N in a single run, for any value of N. Such an approach is generalizable to the reproduction of exponential sums of any order j, with subsequent reduction of the number of resources compared to the past realizations.

Moreover, in this procedure, we will not take into account the term with $m = 0$ in the truncated exponential sum (1), because it corresponds to a null phase, no matter if the trial factor ℓ is a factor or not.

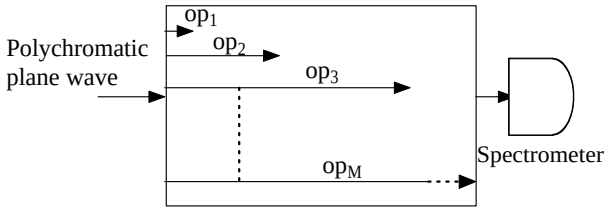

FIG. 1: Theoretical model of a generic M-path optical interferometer, where $op_m \equiv m^j N u$ is the length of the m_{th} optical path with $m = 1, 2, ..., M$. The optical paths are represented by arrows, which length increase quadratically, in the case of Gauss sums ($j = 2$). The incoming electromagnetic field is given by a polychromatic plane wave and the spectrum of the outgoing field, given by the interference of all the M optical paths, is measured by a spectrometer.

Our procedure is based on two basic simple ideas. The first idea consists of the use of an M-path optical interferometer. Such an interferometer needs to be able to reproduce, for a definite wavelength λ, M spatial modes with phase terms of order j and add them coherently in order to reproduce the truncated exponential sums. The second basic idea consists of exploiting the spectrum of the incoming light in order to reproduce all the possible trial factors in a single run for any value of N, measuring the intensity of the outgoing light as a function of the wavelength.

We will now explain, in detail, the physical working principle behind the two main ideas stated above.

In general, an M-path optical interferometer (see Fig. 1), interacting with an incoming polychromatic plane wave, allows the coherent superposition of M electromagnetic phase terms (modes). The optical phase of the generic term, associated with the wavelength λ and with the m^{th} optical path, with $m = 1, ..., M$, is given by:

$$\phi_m(\lambda) \doteq 2\pi \frac{op_m}{\lambda}, \qquad (2)$$

where

$$op_m \doteq n_m d_m \qquad (3)$$

is the m^{th} optical path, n_m is the index of refraction of the material in the path, and d_m is the length of the path.

The truncated exponential sum (1), not including the term $m = 0$, is reproduced by the coherent superposition of all the M phase terms in Eq. (2), if the following conditions are satisfied:

$$\phi_m(\lambda) \equiv 2\pi m^j \frac{N}{\ell}, \tag{4}$$

for each $m = 1, 2, ..., M$.

In order to achieve this goal, we use a polychromatic source so that we can exploit all the spectrum of the incoming light in order to reproduce all the possible trial factors at the same time, through the following correspondence:

$$\lambda \equiv \ell u, \tag{5}$$

where u is an appropriate unit of measurement of length. Such a unit is chosen so that all the possible trial factors can be experimentally reproduced exploiting all the range of Fourier modes λ emitted by a polychromatic source S, with associated intensity $|E_S(\lambda)|^2$ large enough to be measured. The other important step consists in varying the M optical paths in Eq. (3) in order to satisfy the following conditions:

$$op_m \equiv m^j N u, \tag{6}$$

for each $m = 1, 2, ..., M$.

If both Eq. (5) and Eq. (6) are satisfied, the magnitude of the outgoing electromagnetic field is given by the superposition of all the M exponential phases in Eq. (4), for each of the Fourier modes $\lambda \equiv \ell u$ in the spectrum of the source.

At this point, we can use a spectrometer in order to measure the intensity of the outgoing electric field

$$|E_\lambda(M, N, j)|^2 \equiv |E_S(\lambda)\mathcal{A}_N^{(M,j)}(\lambda)|^2, \tag{7}$$

as a function of the wavelength $\lambda \equiv \ell u$; where $E_S(\lambda)$ is the amplitude associate to the Fourier mode λ emitted by the source and $\mathcal{A}_N^{(M,j)}(\lambda)$ is given by Eq. 1, with $l = \frac{\lambda}{u}$. Knowing the spectrum of emission $|E_S(\lambda)|^2$ of the source, it is easy to extrapolate the modulo squared $|\mathcal{A}_N^{(M,j)}(\lambda)|^2$ of the truncated exponential sum versus the wavelength $\lambda \equiv \ell u$. The factors correspond to the wavelengths which allow constructive interference and so maxima in the extrapolated intensity spectrum.

It is important to point out that our factorization approach allows for the first time to achieve two important goals. The first one is the implementation of two independent parameters corresponding to N and ℓ, respectively. Moreover this approach allows us to determine the factors of N in a single run of the experiment. For the first time, in an exponential sum approach to factorization, the ratio $\frac{N}{\ell}$ is not known a priori and it is not necessary to run the experiment for all the possible trial factors.

At this point, it is important to point out some experimental aspects associated to the conditions in Eq. (5) and Eq. (6). Both the optical paths and the wavelengths in the spectrum of the outgoing field need to be measured with the resolution of $1u$. So, experimentally speaking, the larger is the unity of measurement u, the smaller is the necessary resolution in the actual experimental realization. But, at the same time, increasing the value of u, the bandwidth of the optical spectrum necessary to cover all the trial factors increases by the same factor. Another important point to take into account is that the less the resolution of the spectrometer, the larger is the number of measurements we need to perform in the different ranges of the spectrum of the light source, in order to cover all the trial factors.

Now we present a simple factorization algorithm, based on the factorization approach described so far. Such an algorithm can be implemented in four different steps. The first one consists of choosing a particular wavelength $\overline{\lambda}$, which corresponds to a given number $\overline{N} \equiv \frac{\overline{\lambda}}{u}$ to factorize. The second step consists of varying the optical paths in Eq. (3) as long as the electromagnetic phase terms in Eq. (2) satisfy the following condition:

$$\phi_m(\overline{\lambda}) = 2\pi m^j, \tag{8}$$

with $m = 1, 2, ..., M$.

In the third step, we consider a polychromatic plane wave interacting with the generic M-path interferometer in Fig. 1, keeping fixed the optical paths determined in the previous step. In this case, each wavelength λ corresponds to a particular set of phases (2), which can be written in the following way:

$$\phi_m(\lambda) = 2\pi m^j \frac{\overline{\lambda}}{\lambda}, \tag{9}$$

with $m = 1, 2, ..., M$. The phases (9) are the exponential sum phases, associated with the number $\overline{N} \equiv \overline{\lambda}$ to factorize and the generic trial factor ℓ, given by Eq. (5).

In the fourth step of the algorithm, we implement the factorization of a generic number N, choosing a parameter α such that:

$$N = \alpha\overline{N} \equiv \alpha\frac{\overline{\lambda}}{u}. \tag{10}$$

In order to achieve this goal, it is possible to rescale the condition $\lambda \equiv \ell u$, imposing the new condition $\lambda \equiv \ell\frac{u}{\alpha}$. Unfortunately, this approach is limited by the achievable range of wavelengths in the spectrum of emission of the source. Another possible approach, independent from the spectrum of emission of the source, consists of multiplying the lengths of all the M optical paths, found in the second step, by a factor α. In this way, we can factorize any number N using a simple rescaling procedure.

Let us now describe how to experimentally realize our factorization procedure. In order to satisfy the condition (6), we need to be able to manipulate either the indexes of refraction n_m associated with the M optical

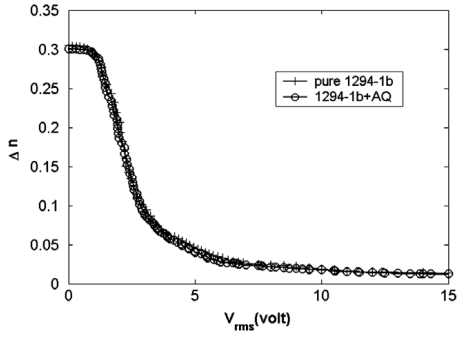

FIG. 2: Voltage-birefringence curve, at $\lambda = 632.8nm$, $T = 24°C$, for: (1) a pure nematic liquid crystal (NLC) mixture, denoted as $1294 - 1b$, of thickness $d = 8.08\mu m$; and (2) 0.2% of antraquinone derivative(AQ) dissolved in $1294 - 1b$, with thickness $d = 7.82\mu m$[9].

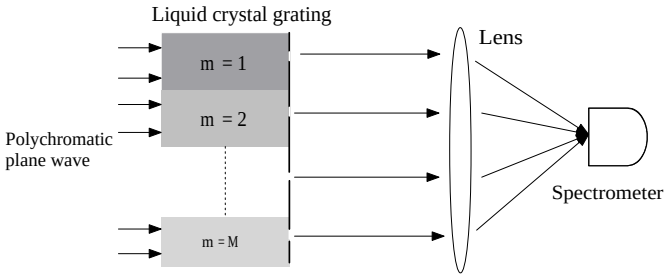

FIG. 3: Liquid crystal interferometer: a polychromatic plane wave, in the ordinary mode, interacts first with a liquid crystal grating, with M regions and respective slits, and at the end with a lens. A spectrometer measures the intensity of the light as a function of the wavelength in the focal plane of the lens.

paths (3) in the interferometer or the lengths of the M paths. The first approach can be implemented by using a liquid crystal grating. In the second approach, instead, we introduce a generalized symmetric Michelson interferometer.

Let us analyze the first approach. First, we will describe an interesting property which makes liquid crystals able to satisfy the conditions (4) for the reproduction of truncated exponential sums. When we apply a variable voltage V to a liquid crystal cell, interacting with an incoming plane wave, we can observe the voltage dependence of the birefringence $\triangle n \doteq n_e - n_o$ [10] of the liquid crystal (see, for example, Fig. 2). In particular, there is a limited range of potentials in which the transmission, and so the liquid crystal index of refraction, has a well defined dependence on the applied voltage. Such a definite behavior turns out to be a good tool in order to reproduce the terms m^j, with $m = 0, 1, ..., M$, in Eq. (1).

The M terms in the truncated exponential sum correspond, respectively, to M different regions in a liquid crystal cell with the same thickness $d_m \equiv d$.

The basic experimental setup is showed in Fig. 3: an incoming polychromatic plane wave, in the ordinary mode, interacts with a liquid crystal grating with M slits. Such a grating consists of M liquid crystal regions, with M different variable applied voltages V_m, with $m = 1, 2, ..., M$, and a slit at the end of each region.

So, when the incoming polychromatic plane wave interacts with the liquid crystal grating, it gives rise to M different electromagnetic phase terms, which can be manipulated in an appropriate way, varying the applied voltages V_m and so the associated indexes of refraction. Such terms superpose coherently in the focal point of a lens.

At this point, it is very easy to implement the algorithm previously described in order to reproduce exponential sums.

Of course, in the experimental realization of such approach, we need to take into account the dispersion associated with the broadband spectrum of the source. Such problem can be overcome performing several measurements in different ranges of the spectrum of the light source such that the relative dispersion in each range is negligible.

It is also important to point out that the larger the maximum achievable optical path, the larger is also the maximum achievable truncation parameter M in Eq. (8). Unfortunately, in the liquid crystal approach, the maximum range of variation of the optical paths is limited by the thickness d of the liquid crystal cells and by the birefringence, calculated when no voltage is applied [11]. Consequently, both these parameters determine the maximum number of terms in the truncated exponential sum and the maximum range of possible number N we can factorize.

We have seen one possible way of varying the optical paths, in an M-path interferometer, in order to obtain phase terms of order j. A second way to achieve the same result is varying, in free space, the path lengths d_m in Eq. (3). In this case, we do not encounter any problem associated with dispersion. So we can determine all the factors at the same time, exploiting all the spectrum of the incoming light [12].

This approach can be implemented exploiting the multi-path interference in a generalized symmetric Michelson interferometer in free space: the usual two-path Michelson interferometer is generalized, in a symmetric way, to a M-path interferometer, using $M - 1$ beam splitters. In Fig. (4) we have represented, for simplicity, the case $M = 4$ (obviously such an approach can be extended to a generic M). In this case, the four interfering optical paths can be varied arbitrarily by translating the mirrors M_1, M_2, M_3 and M_4, respectively. Our factorization algorithm can be easily implemented using such an interferometer, giving all the factors of any number N in a single run. Moreover, because the lengths of the interfering paths can be in principle as large as we

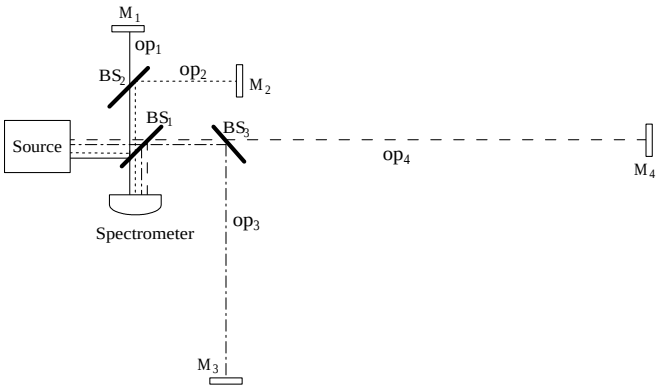

FIG. 4: Generalized symmetric M-path Michelson interferometer for the realization of exponential sum with truncation parameter $M = 4$. The usual two-paths Michelson interferometer is generalized to an M-path interferometer, using $M - 1$ beam splitters. The $M = 4$ interfering optical paths, indicated with dashed, dashed-dotted, continuous, and dotted lines can be varied by moving longitudinally the mirrors M_1, M_2, M_3 and M_4, respectively, in order to satisfy the condition (6).

want, there is no limit to the maximum achievable truncation parameter M and order j of the exponential sum we want to reproduce. This is another aspect in favor of this approach, rather than the one based on a liquid crystal grating. On the other hand such an interferometer, despite the liquid crystal grating, is more difficult to align and to make stable, especially for large values of M. Anyway, these challenges can be experimentally overcome, and the Michelson interferometer approach turns out to be experimentally reliable, especially if we consider that for exponential sums of high order j, only a relatively small number M of interfering paths is necessary ($M \sim \sqrt[2j]{N}$).

In conclusion, we have shown how an optical interferometer would allow the factorization of a large number N in a single run of a simple algorithm, for any value of N. Our algorithm is reliable, in general, for reproducing truncated exponential sums of any order j, with a consequent reduction of experimental resources with respect to Gauss sums. We have shown how our approach allows us to determine, for each value of N, the discrete spectrum of the associated truncated exponential sum, as a function of all the possible trial factors. In general, such an approach goes beyond a discrete analysis of exponential sums. In fact, new interesting tools in the factorization procedure can be provided exploiting the physics and mathematics behind the continuous interference spectrum of our optical interferometer approach. Moreover, we have described two different kinds of optical interferometers which can be used in this approach: a liquid crystal grating and a generalized Michelson interferometer. Two separate experiments based on both schemes are in progress and the results will be soon available in a forthcoming paper. We are also considering the use of the same approach for the realization of truncated exponential sums with a number of terms $M' < M$, randomly chosen among the total M terms in Eq. 1.

The authors thank J. Franson, T. Pittman, M. H. Rubin, W. Schleich and T. Worchesky for useful suggestions and stimulating discussions. This research was partially supported by the US AFOSR. During the preparation of this paper, we became aware of a related work by A. Rangelov, connected with the use of a Michelson interferometer.

[1] R. Rivest, A. Shamir, and L. Adlemanencryption, Communications of the ACM **21(2)**, 120-126 (1978).
[2] W. Merkel, I.Sh. Averbukh, B. Girard, G.G. Paulus, and W.P. Schleich, Fortschr. Phys. **54**, 856 (2006)
[3] M. Stefanak, W. Merkel, W.P. Schleich, D. Haase, and H. Maier, New J. Phys **9**, 370 (2007)
[4] M. Stefanak, W. Merkel, W.P. Schleich, D. Haase, and H. Maier, J. Phys. A: Math. Theor. **41**, 304024 (2008)
[5] M. Mehring, K. Müller, I.Sh. Averbukh, W. Merkel, and W.P. Schleich, Phys. Rev. Lett. **98**, 120502 (2007).
[6] T.S. Mahesh, N. Rajendran, X. Peng, and D. Suter, Phys. Rev. A **75**, 062303 (2007).
[7] M. Gilowsky, T. Wendrich, T. Muller, Ch. Jentsch, W. Ertmer, E.M. Rasel and W.P. Schleich, Phys. Rev. Lett. **100**, 030201 (2008).
[8] D. Bigourd, B. Chatel, W.P. Schleich, and B. Girard, Phys. Rev. Lett. **100**, 030202 (2008).
[9] A. Jafari, H. Tajalli, and A. Ghanadzadeh, Optics Communications **266**, 207-213 (2006).
[10] n_e is the index of refraction associated to the extraordinary mode, while n_o is the index of refraction associated to the ordinary mode.
[11] For example, the liquid crystals represented in Fig. 2 have a birefringence $\triangle n_{V=0} \sim 0.3$, calculated when no voltage V is applied.
[12] The number of measurement in the actual factorization procedure depends only on the resolution of the spectrometer, as pointed out previously.